Custom Lightweight Discovery Protocol (CLDP) Specification

Date: March 31, 2025
Course: CS39006: Networks Laboratory
Assignment: 7 - Design and Implementation of CLDP

G SAI SHASANK

22CS10025

1. Overview

The Custom Lightweight Discovery Protocol (CLDP) is designed for a closed network environment to enable nodes to announce their presence and query other nodes for specific application-level metadata. This protocol operates at the IP layer using raw sockets, bypassing traditional transport-layer protocols like TCP or UDP. CLDP supports three message types: HELLO, QUERY, and RESPONSE.

2. Protocol Design

2.1 Message Types

CLDP defines the following message types:

1. 0x01: HELLO
   Used by nodes to announce their active status.
2. 0x02: QUERY
   Sent by clients to request metadata from active servers.
3. 0x03: RESPONSE
   Sent by servers in response to a QUERY message, containing requested metadata.

2.2 Custom Header Format

Each CLDP message contains a custom header with the following fields:

Field Name	Size (Bytes)	Description
Message Type	4	Indicates the type of message (HELLO, QUERY, or RESPONSE).
Payload Length	2	Length of the payload in bytes (excluding headers).
Transaction ID	4	Unique identifier for tracking requests and responses.
Reserved	1	Reserved for future use (set to 0).
Checksum	2	Checksum for error detection in the custom header and payload.
System Time	4	Timestamp indicating when the message was created.
Hostname Length	2	Length of the hostname string in bytes.
CPU Load	4	CPU load (1-minute average).
Memory Usage	4	Memory usage as a percentage of total memory.

2.3 Message Layout

The layout of a complete CLDP message is as follows:

Custom header	IP Header	Hostname String	Payload

- Custom Header: Contains protocol-specific fields as described above.
- IP Header: Includes source and destination IPs, protocol number (253), etc.
- Hostname String: Optional field containing the hostname of the sender.
- Payload: Optional data based on the message type.

3. Metadata Supported

The following application-level performance counters are supported:

1. Hostname: The name of the system sending the message.
2. CPU Load: The system's CPU load (1-minute average).
3. Memory Usage: The percentage of memory currently in use.
4. System time : The timestamp of server at that time

4. Message Workflow

4.1 HELLO Message

- Broadcasted by servers every 10 seconds to announce their active status.
- Contains metadata such as hostname, CPU load, and memory usage.

4.2 QUERY Message

- Sent by clients to request metadata from all active servers.
- Requests all three supported metadata fields: hostname, CPU load, and memory usage.

4.3 RESPONSE Message

- Sent by servers in response to QUERY messages.
- Contains requested metadata along with the server's system time.

5. Implementation Details

5.1 Raw Socket Programming

- CLDP uses raw sockets (AF_INET, SOCK_RAW) with a custom protocol number (253).
- IP headers are manually crafted using the IP_HDRINCL socket option.

5.2 Packet Crafting

- The IP header includes fields such as source/destination IPs, TTL, protocol number, etc.

5.3 Checksum Calculation

- A checksum is calculated over the custom header and payload for error detection.

6. Demonstration Scenario

1. Multiple servers broadcast HELLO messages every 10 seconds.
2. A client sends a QUERY message to all active nodes via broadcast.
3. Servers respond with RESPONSE messages containing their hostname, CPU load, memory usage, and system time.

7. Example Use Case

HELLO Message Example

Message Type: 0x01

Payload Length: 0

Transaction ID: Randomly generated

Reserved: 0

Checksum: Calculated over header

System Time: Current timestamp

Hostname Length: Length of hostname string

CPU Load: Current CPU load

Memory Usage: Current memory usage percentage

QUERY Message Example

Message Type: 0x02

Payload Length: 0

Transaction ID: Incremental counter

Reserved: 0

Checksum: Calculated over header

System Time: Current timestamp

Hostname Length: Client's hostname length

CPU Load & Memory Usage: Not applicable for QUERY messages

RESPONSE Message Example

Message Type: 0x03

Payload Length: Metadata size

Transaction ID: Same as QUERY message ID

Reserved: 0

Checksum: Calculated over header + payload

System Time: Server's current timestamp

Hostname Length: Server's hostname length

CPU Load & Memory Usage: Included in payload

8. Assumptions and Limitations

- The protocol is designed for a closed network environment with trusted nodes.
- Raw sockets require elevated privileges; programs must be run with sudo.
- The implementation does not handle fragmented packets or retransmissions.